Hindawi
Complexity
Volume 2020, Article ID 8868884, 16 pages
https://doi.org/10.1155/2020/8868884

Research Article

Improved 2D Discrete Hyperchaos Mapping with Complex Behaviour and Algebraic Structure for Strong S-Boxes Generation

Musheer Ahmad[1] **and Eesa Al-Solami**[2]

[1]*Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India*
[2]*Department of Information Security, University of Jeddah, Jeddah 21493, Saudi Arabia*

Correspondence should be addressed to Musheer Ahmad; musheer.cse@gmail.com

Received 30 September 2020; Revised 7 December 2020; Accepted 11 December 2020; Published 23 December 2020

Academic Editor: Jesus M. Muñoz-Pacheco

This paper proposes to present a novel method of generating cryptographic dynamic substitution-boxes, which makes use of the combined effect of discrete hyperchaos mapping and algebraic group theory. Firstly, an improved 2D hyperchaotic map is proposed, which consists of better dynamical behaviour in terms of large Lyapunov exponents, excellent bifurcation, phase attractor, high entropy, and unpredictability. Secondly, a hyperchaotic key-dependent substitution-box generation process is designed, which is based on the bijectivity-preserving effect of multiplication with permutation matrix to obtain satisfactory configuration of substitution-box matrix over the enormously large problem space of 256!. Lastly, the security strength of obtained S-box is further elevated through the action of proposed algebraic group structure. The standard set of performance parameters such as nonlinearity, strict avalanche criterion, bits independent criterion, differential uniformity, and linear approximation probability is quantified to assess the security and robustness of proposed S-box. The simulation and comparison results demonstrate the effectiveness of proposed method for the construction of cryptographically sound S-boxes.

1. Introduction

The modern secure communication based on block ciphers plays a significant role. It provides a way to stay secure against unauthorized access and tampering in an insecure communication channel. The usage of cryptographic primitives such as data encryption methods, hash functions, and pseudorandom number generators depends upon the area of applications [1–4]. A block cipher is a symmetric encryption mechanism that relies on one private key for successful encryption and decryption of data at the sender side and at the receiver side, respectively. It takes an input block of size n bits and a key of size k bits and produces an output of n bits during the process of encryption and decryption. There exists a number of block cryptosystems, and some of the well-known are Data Encryption Standard (DES), Advanced Encryption Standard (AES), international data encryption algorithm (IDEA), and KASUMI. These block cryptosystems play a crucial role in multimedia security [5]. The architecture of secure block ciphers consists of two vital components, namely, substitution-box at the substitution layer and permutation-box at the permutation layer, which in combination bring the effect of necessary confusion and diffusion in the system. The aim of substitution-box (S-box) is to produce desired confusion between the ciphertext and the key, whereas the permutation-box (P-box) is needed to spread the inputs linearly and randomly for the diffusion [6].

The substitution layer in a symmetric-key cryptosystem is meant to perform the process of data substitution with the help of S-boxes. Substitution-boxes are the only components in block ciphers that add nonlinearity to the operation of the cryptosystem. Substitution-boxes are decisive components of symmetric-key algorithms as they are the only nonlinear transformation that transforms inputs to outputs in some nonlinear fashion [7]. They are sort of nonlinear mappings that substitute a set of input bits of size n-bits with a different set of bits called output bits as $S\colon \{0,1\}^n \longrightarrow \{0,1\}^m$, where n

represents the number of input bits for $n \times m$ S-box and m represents output bits from S-box after substitution. An $n \times m$ S-box can be generated as a lookup table with 2^n words of m-bits each. S-boxes are also termed as the vectorial Boolean functions or multiple-input multiple-output Boolean functions. This means that an $n \times m$ S-box consists of m different component Boolean functions as $S[g_{m-1}, g_{m-2}, \ldots, g_1, g_0]$, where each $g_i\,(0 \le i < m)$ is Boolean function in n variables, that is, $g_i\,(0 \le i < m)$: $\{0,1\}^n \longrightarrow \{0,1\}$ [8]. Particularly, the scenario when $n = m$ corresponds to $n \times n$ bijective S-boxes in which there exists a one-to-one mapping from input domain to output domain; that is, each input of n-bit long uniquely maps to an n-bit long output. There exist a vast number of bijective S-boxes for $n = 8$ whose count is 256!, which is more than 10^{506} [9]. Thus, it is challenging for the cryptographers to construct and find cryptographically strong S-boxes configurations out of this vast state space. The cryptographic strength of S-box decides the security of block ciphers. If the S-box is weak, then the resulting cryptosystem will have high linearity and can be easily broken. S-boxes also make the block ciphers powerful and robust to resist linear and differential cryptanalytic attacks [10].

In literature, some significant research efforts have been made to develop substitution-boxes with good measures of desirable cryptographic properties. In [11], Özkaynak and Özer gave a method by exploring the trajectories of 3D Lorenz chaotic system, which determined 8×8 S-box with satisfactory security features. In [12], the authors explored the features of six-dimensional hyperchaotic system and artificial bee colony optimization approach to generate an optimized configuration of S-box. Çavuşoğlu et al. in [13] investigated the dynamical characteristics of new scaled version 3D chaotic Zhongtang system for S-box generation. Ahmad et al. in [14] also investigated an artificial bee colony optimization and 1D chaotic logistic map-based method to construct an S-box which showed better cryptographic features and S-box reported in [12]. Alzaidi et al. reported a sine-cosine optimization and new 1D chaotic map-based S-box construction mechanism in [15]. Wang et al. in [16] suggested a simple 8×8 S-box generation algorithm with the help of a new 3D continuous chaotic system which has infinite equilibrium points. In [17], Zhang et al. studied the dynamics of fractional-order logistic map and designed an S-box construction method with consistent security performance which found application for image encryption. Lambic proposed a new discrete-space 1D chaotic map using the concept of multiplication of integer numbers and circular shift and gave an 8×8 S-box generation application for security usages in [18]. Recently, Gao et al. presented a new way of constructing S-boxes by using the algebraic action of modular groups PSL $(2, Z)$ on a particular projective line in [19]. The obtained S-box met all the performance criteria well and was deemed suitable for encryption applications. Hematpour and Ahadpour investigated strong chaotic nonlinear map for performance improvisation of particle swarm optimization, which was then executed to optimize the S-box for high nonlinear property in [20]. Their examination and application of improved PSO resulted in some good set of S-boxes with acceptable cryptographic features. For some recent S-box generation methods, the readers are referred to [21–29].

Chaos-based cryptography has coveted to design and use the chaotic maps for the development of security methods such as multimedia encryption algorithms, watermarking, steganography, hash functions, substitution-box design, pseudorandom number generators, and authentication protocols [4, 30–37]. The robustness of these cryptographic primitives is significantly based on the dynamical characteristics of employed chaotic maps. The chaotic maps with frail performance may lead to weak security effect offered by the cryptographic primitive based on weak chaotic maps or systems [38]. But most of them are found to hold one or other limitations that restricted their usage to develop a strong cryptographic application. Utilization of chaotic maps with frail performance may threaten the security of cryptographic system and make it susceptible to attacks [38, 39]. They have the problems of limited chaotic range and behaviour, nonuniform coverage of chaotic attractor in phase space, low Lyapunov exponent, low complexity, etc. [40, 41]. This motivates to construct chaotic maps that should possess better and more rich dynamical features than conventional chaotic maps [35, 38, 40–43]. Consequently, an improved 2D hyperchaotic map is designed, which has significantly better dynamical characteristics compared to existing 2D chaotic map. Some of the significant contributions presented in this paper are as follows:

(1) An improved 2D discrete hyperchaotic map is suggested, which exhibits rich dynamical features in terms of Lyapunov exponents, bifurcation, entropy, complexity, etc.

(2) A chaotic permutation matrix based novel approach is presented to search a suitable configuration of substitution-box. The multiplication of permutation matrix with input S-box preserves the bijectivity property of S-box.

(3) A strong and persuasive algebraic group-theoretic structure has been found experimentally, whose actions further elevated the cryptographic strength of the S-box.

(4) The security assessment against benchmarking parameters is done, which shows excellent performance of proposed S-box generation method.

(5) The security strength of obtained S-box is compared and analyzed with some recently investigated S-boxes studies to make evident the standout features of the proposed method.

The structure of the rest of the paper is maintained as follows: The model of an enhanced 2D chaotic map and its dynamical analyses is discussed in Section 2. The application of developed hyperchaos mapping for permutation matrix based proposed 8×8 S-box generation algorithm and algebraic group action is described in Section 3. Section 4 reports the performance assessments and analyses of proposed S-box and its comparison with existing S-boxes. The conclusion of the research works done in this paper is mentioned in Section 5.

2. 2D Discrete Hyperchaos Mapping

The dynamics of the proposed 2D discrete hyperchaotic mapping are governed by the mathematical form shown in the following equation:

$$\left.\begin{array}{l} x_{n+1} = \left[r^2 x_n + k\sin(\pi x_n)\left(a - h(x_n, y_n, b) + b\tan(x_n + y_n)\right)\right]\mathrm{mod}\,(1) \\ y_{n+1} = \left[r^2 y_n + k\tan(x_n + y_n)\left(a - h(y_n, x_n, b) + b\sin(\pi y_n)\right)\right]\mathrm{mod}\,(1) \end{array}\right\}, \quad (1)$$

where $h(x_n, y_n, b) = (bx_n/x_n^3 - \pi y_n)$ and $x_n, y_n \in (0,1)$ are chaotic state variables of the map after n iterations. It also includes the parameters a, b, $k > 0$, and $r > 1$. Existence of large number of map's parameters extends the key space when the map is incorporated in any cryptographic applications which make the brute-force attacks impractical. The initial values of x_0 and y_0 along with setting of their parameters decide the future trajectory of the map. The default setting in all computer simulations and experiments related to proposed 2D map (1) is as follows: $x_0 = 0.11$, $y_0 = 0.12$, $a = 1.5$, $b = 0.5$, $k = 2$, and $r = 3$.

The mathematical form of 2D logistic chaotic map is as follows [44]:

$$\left.\begin{array}{l} x_{n+1} = r(3y_n + 1)x_n(1 - x_n) \\ y_{n+1} = r(3x_n + 1)y_n(1 - y_n) \end{array}\right\}, \quad (2)$$

where r is its control parameter. The 2D logistic map exhibits its chaotic behaviour when parameter r lies in [1.11, 1.15] or [1.18, 1.19].

The 2D Henon chaotic map is described through the following equation [45]:

$$\left.\begin{array}{l} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{array}\right\}, \quad (3)$$

where a and b are its system parameters that decide its dynamical behaviour. It is known that 2D Henon map shows chaotic behaviour for $b = 0.3$ and a lies in [1.06, 1.22] or [1.27, 1.29] or [1.31, 1.42].

The 2D sine-logistic modulation map (SLMM) suggested and investigated in [46] has the following mathematical form:

$$\left.\begin{array}{l} x_{n+1} = a\left(\sin(\pi y_n) + 3\right)x_n(1 - x_n) \\ y_{n+1} = a\left(\sin(\pi x_{n+1}) + 3\right)y_n(1 - y_n) \end{array}\right\}, \quad (4)$$

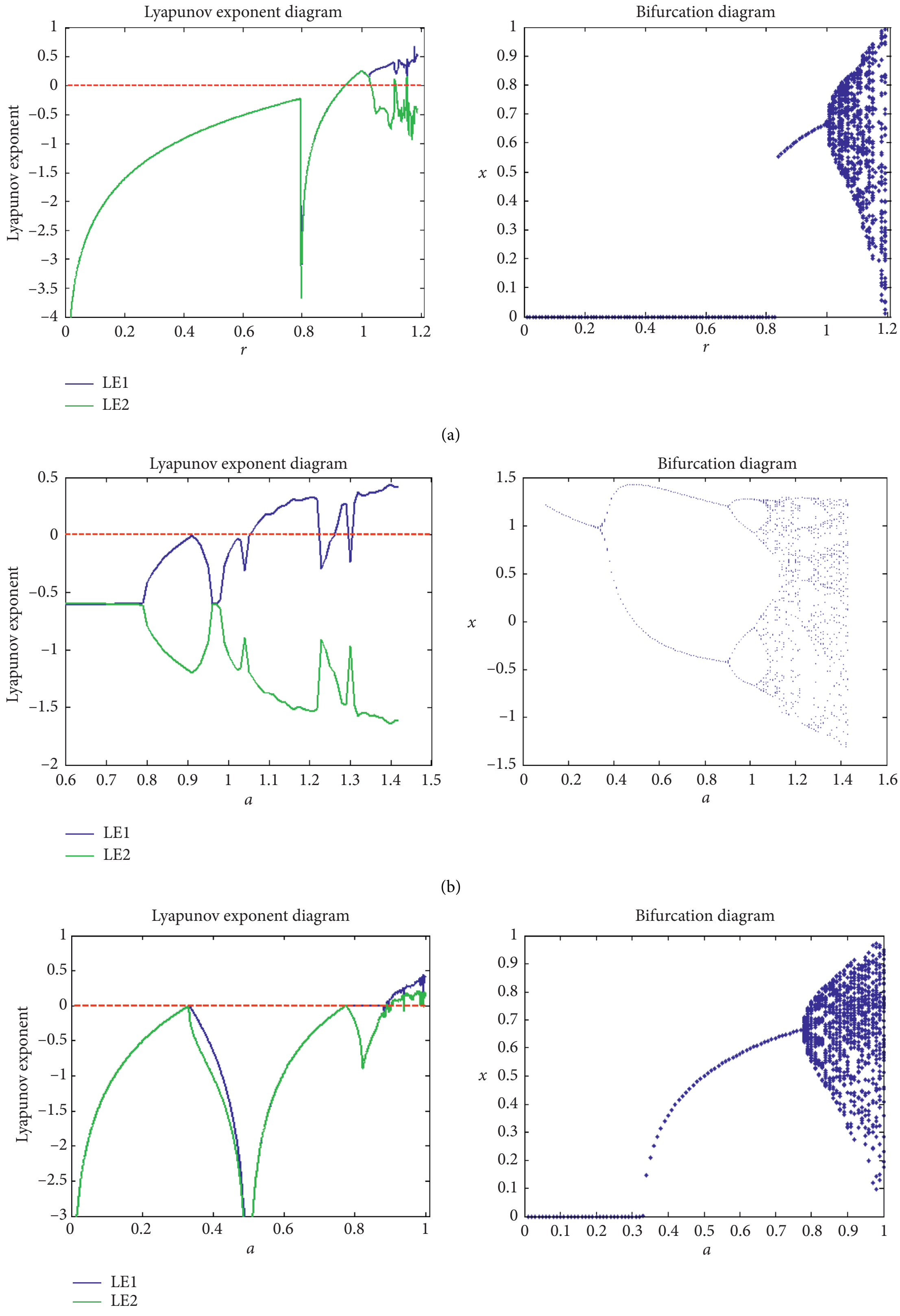
where a is the system's bifurcation parameter. Regarding the 2D SLMM map, it was studied that it exhibits chaotic phenomenon when a lies in [0.87, 1] but shows hyperchaotic behaviour when the parameter lies in [0.905, 1]. In what follows, the dynamics of the proposed map (1) are analyzed and compared with three mentioned 2D chaotic discrete maps: logistic map, Henon map, and SLMM map.

2.1. Lyapunov Exponents. Lyapunov exponent (LE) is a quantitative measure used to determine the degree of chaotic behaviour of a dynamic system. It is a commonly accepted metric that describes the separation between two trajectories starting from extremely close initial points [47]. Mathematically, Lyapunov exponents for a dynamical map $x_{i+1} = f(x_i, y_i)\&y_{i+1} = g(x_i, y_i)$ are computed as

$$\left.\begin{array}{l} \mathrm{LE}_1 = \lim\limits_{n\longrightarrow\infty}\left[\dfrac{1}{n}\sum\limits_{i=1}^{n}\log\left|\dfrac{d}{\mathrm{d}x}(x_{i+1})\right|\right] \\ \\ \mathrm{LE}_2 = \lim\limits_{n\longrightarrow\infty}\left[\dfrac{1}{n}\sum\limits_{i=1}^{n}\log\left|\dfrac{d}{\mathrm{d}y}(y_{i+1})\right|\right] \end{array}\right\}, \quad (5)$$

A positive value of Lyapunov exponent indicates chaotic nature between the two trajectories; that is, no matter how close the initial distance is, trajectories will diverge exponentially over time making them unpredictable. Hence, a larger value of LE indicates superior chaotic phenomenon of the system [40]. The Lyapunov exponents of the proposed chaotic map for different values of parameters k and r are shown in Figure 1. It can be seen that the enhanced map shows chaotic phenomenon for complete range of $k, r \in (0, 10)$. Particularly, a hyperchaotic nature of map (1) is evident from Figures 1(d) and 1(e) as both exponents are found to possess positive values over whole specified range of bifurcation parameters k and r. Moreover, it is worth noting that a similar kind of behaviour is experienced for larger of values of both parameters of proposed enhanced map (1). Specifically, the exponents get bigger for higher values of parameters k and r, thereby reflecting the higher divergence of orbits and complicated nature of existence of chaos. Since the 2D map (1) has both LE positives that indicate a KY dimension of proposed map as 2.0, The Lyapunov exponents for the proposed 2D map are also analyzed by varying the parameters k and r simultaneously, and the obtained diagrams are shown in Figure 2. The diagrams confirm the existence of hyperchaos phenomenon of the proposed map for a wide range of both parameters. For comparison, the Lyapunov values of proposed map for mentioned settings are listed in Table 1 and we found fairly larger LE values obtained from our 2D chaotic map than some existing 2D discrete chaotic maps. Hence, Figure 1 shows a richer dynamical behaviour and high sensitivity of proposed hyperchaotic map compared to contemporary 2D logistic chaotic map, 2D Henon chaotic map, and 2D SLMM map.

2.2. Bifurcation. Bifurcation analysis is used to quantify regions of chaotic behaviour of a nonlinear dynamic system. Bifurcation is sensitive to control parameters, which, after a special value, cause change in state from fixed to chaotic behaviour indicating that outputs are more random. This shift in phase is known as bifurcation. Bifurcation diagrams are used to visualize the chaotic system behaviour [40]. The

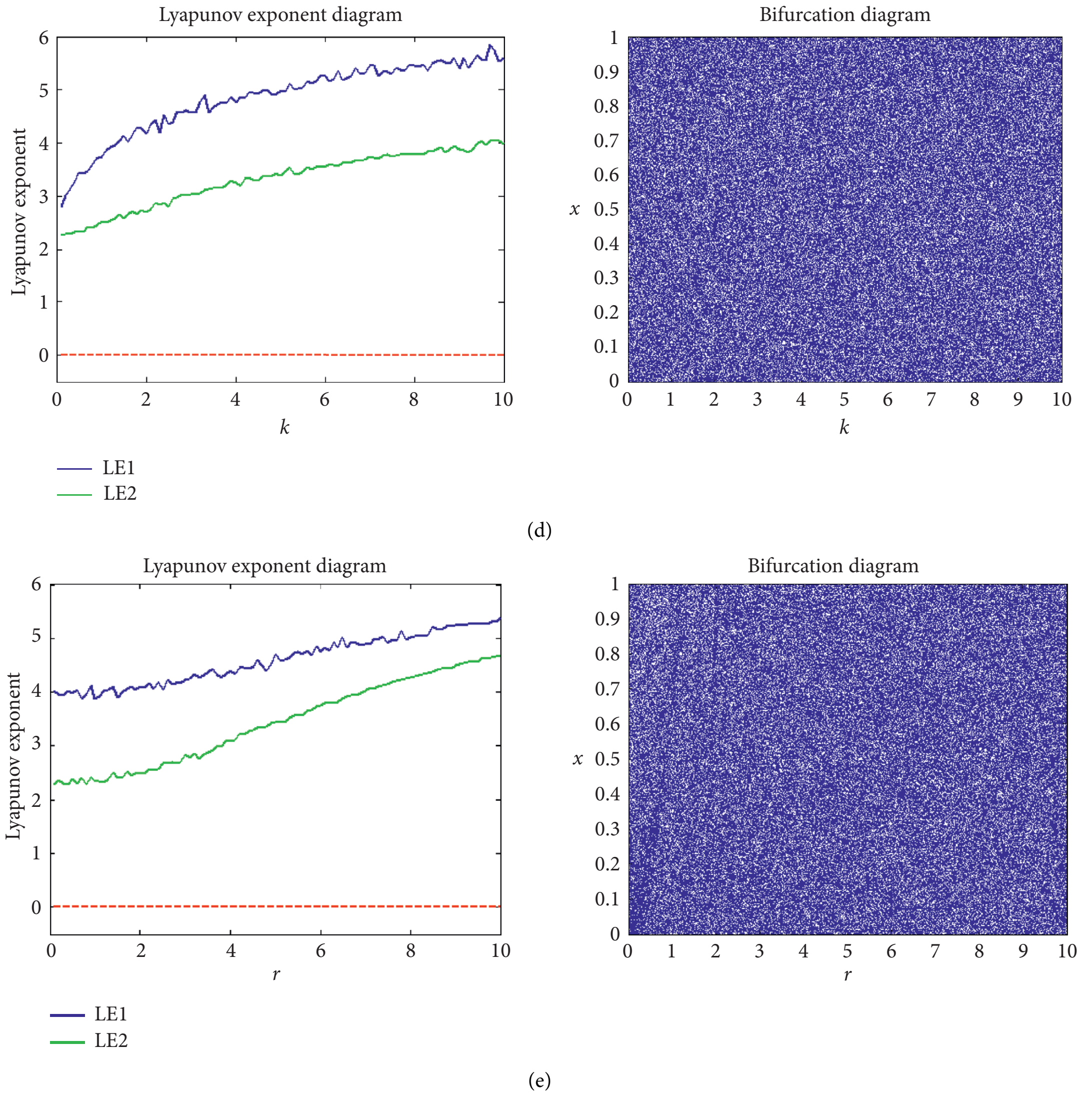


(a)

(b)

(c)

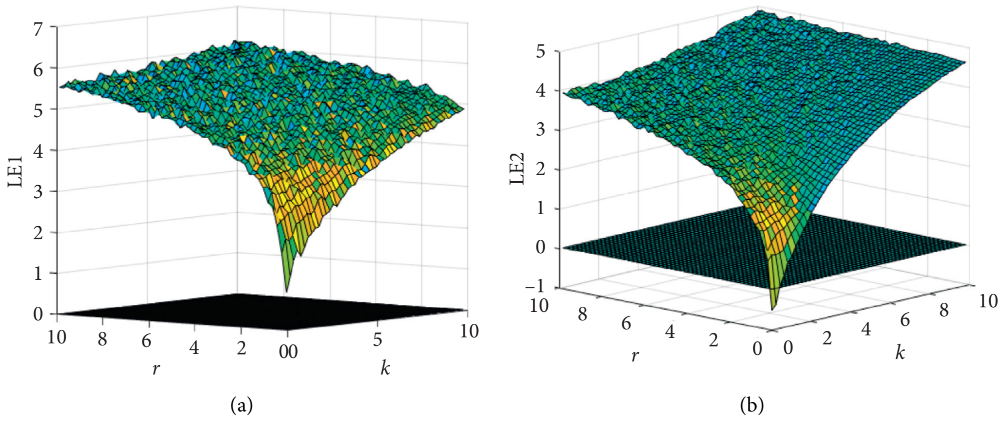
Figure 1: Continued.



(d)

(e)

Figure 1: Lyapunov exponents spectrum for 2D discrete (a) logistic map, (b) Henon map with $b = 0.3$, (c) SLMM map, (d) improved map for parameter k, and (e) improved map for parameter r.



(a)

(b)

Figure 2: Lyapunov exponent diagrams by varying parameters $k, r \in (0, 10]$ simultaneously.

Table 1: Dynamical features comparison of different 2D discrete chaotic maps.

2D chaotic map	MLE	ApEn		Correlation	
		Mean	Max	C1	C2
Logistic map [44]	0.6718	0.0291	0.3118	0.0548	0.0726
Henon map [45]	0.4343	0.1212	0.4784	−0.0123	−0.0121
SLMM map [46]	0.4398	0.1038	0.5986	0.0283	0.01187
Proposed map	5.8579	1.3247	1.3455	−0.0061	−0.0049

bifurcation analysis of the proposed map (1) is investigated for $k, r \in (0, 10]$. The bifurcation plots of different 2D discrete chaotic maps are shown in Figure 1 (right column). It is clear from Figures 1(d) and 1(e) that there do no exist any blank windows or nonchaotic regions in the bifurcation diagram of the proposed map (1). It has been found through simulation that similar bifurcation behaviour exists for both map's parameters $k, r > 0$. The proposed map has pretty better bifurcation behaviour for parameters k and r under system's both variables x and y than bifurcation behaviour of 2D logistic chaotic map, 2D Henon chaotic map, and 2D SLMM map as evident from Figure 1 bifurcation diagrams.

2.3. Time Series Correlation. The X and Y time series obtained from the proposed 2D hyperchaotic map with mentioned settings are shown in Figure 3. In order to show the sensitiveness to small change in initial conditions, different Xc and Yc times series are generated, whose corresponding x_0 and y_0 initial conditions are having a minor difference of $\Delta = 10^{-10}$ only. The respective sequences are shown along with their counterpart series to make it evident that the two are fairly different and nonoverlapping. To quantify the sensitiveness, the correlations between $X\&Xc$ chaotic sequences (denoted as C_1) and Y and Yc (denoted as C_2) are calculated. The correlation between these two pairs of chaotic sequences is provided in Table 1. It is found that the sequences are almost zero correlations as $C_1 = -0.0061$ and $C_2 = -0.0049$, which indicate that the two series are highly deviated and uncorrelated to each other. From Table 1, it is somewhat clear that the correlation coefficients for the sequences from the proposed map are considerably better than coefficients obtained after similar time series analysis for the cases of 2D logistic map, 2D Henon chaotic map, and 2D SLMM map.

2.4. Approximate Entropy. Approximate entropy is a mathematical algorithm created to measure irregularity in time series. It is a nonlinear algorithm that could distinguish between noisy and chaotic time series with small number of data points [48]. A small ApEn value represents deterministic time series, whereas larger value represents randomness, complexity, and unpredictability. Also, a time series tends to have larger ApEn value when patterns are rarely repeated. It has ability to identify intricacy in chaotic behaviour shown by dynamical maps [49]. For an n-dimensional time series $(x_1, x_2, \ldots, x_n)$, ApEn has the following mathematical expression:

$$E(e, t, n) = \Phi^e(t) - \Phi^{e+1}(t), \tag{6}$$

where e denotes the embedding dimension, t is the tolerance, and $\Phi^e(t)$ is defined as

$$\Phi^e(t) = [n - (e-1)\tau]^{-1} \sum_{j=1}^{n-(e-1)\tau} \log\left(\frac{p_j}{n - (e-1)\tau}\right), \tag{7}$$

where τ is the delay in time and p_j is count of k such that $d(x_j, x_k) \leq t$. We calculated the ApEn by varying values of respective bifurcation parameter for existing 2D logistic map, 2D Henon map, 2D SLMM map, and proposed enhanced 2D hyperchaos map; the obtained results are shown in Figure 4. The approximate entropies of different time series obtained by the 2D enhanced chaotic map with same initial conditions are quantified and provided in Table 1. The average ApEn for our enhanced map is found to be around 1.3247, which is sufficient higher than 0.0291, 0.1212, and 0.1038 from existing 2D logistic map, 2D Henon map, and 2D SLMM map, respectively. The obtained ApEn scores justify that the proposed map possesses better complexity and unpredictability compared to existing 2D logistic chaotic map, 2D Henon chaotic map, and 2D SLMM map as evident from Table 1.

2.5. Phase Attractor. The phase diagram to show the coverage of chaotic attractor of the proposed map is provided in Figure 5. It is always significant to analyze the chaotic attractor to know a comprehensive understanding of the dynamics of chaotic maps [50]. We can see in Figure 4 that the attractor covers the entire space like a fractal and does not confine to have a specific shape; rather it covers randomly the complete space even when initial point (x_0, y_0) is fixed anywhere in $[0,1] \times [0,1]$. The phase space of the proposed map is sufficiently complex and perfectly covers the entire region of space compared to the phase attractors of existing 2D logistic chaotic map, 2D Henon chaotic map, and 2D SLMM map.

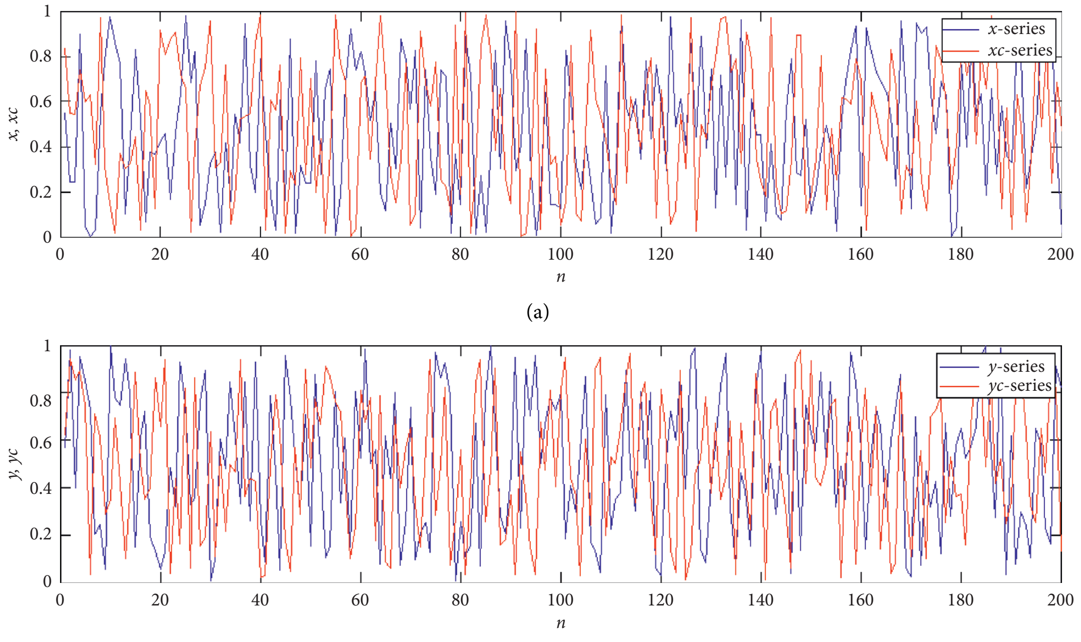
3. Proposed Substitution-Box Generation

This section presents the proposed method of S-box generation. The complete procedure consists of three different phases. In the first phase, an initial bijective 8 × 8 S-box is constructed by using the chaotic values obtained from the improved hyperchaos map (1). The procedure hyperchaos2$d(x, y, a, b, k, r)$ indicates iteration of our proposed hyperchaotic map given in equation (1). The block diagram of the proposed S-box generation method is shown in Figure 6. Meanwhile, the processing steps of different phases of the S-box method are as follows.

Phase 1:

Require: initial conditions of hyperchaos map (2) as $x(0), y(0), a, b, c, k, r$, itr_$n$0, and $s$box = []

Returns: initial S-box A, last x and y chaotic variables



(a)

(b)

Figure 3: Chaotic time series generated from proposed hyperchaotic map: (a) X and Xc sequence; (b) Y and Yc sequence.

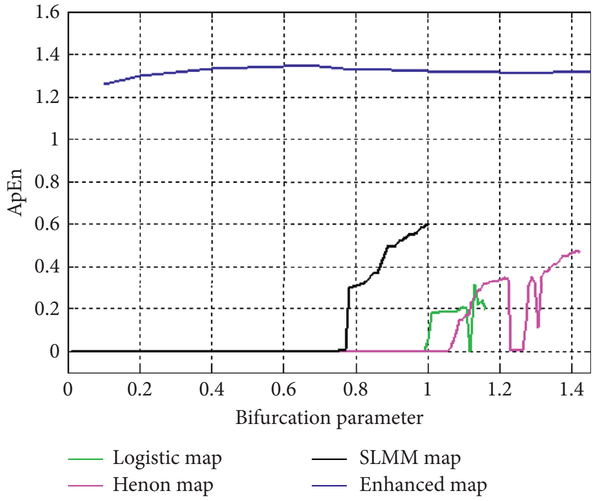


Figure 4: Approximation entropy comparison of 2D chaotic logistic map, Henon map, SLMM map, and proposed hyperchaotic map.

(1) Iterate hyperchaos map (1) for itr_$n0$ times and discard the values to remove transient effect

(2) Further iterate hyperchaos map (1) once and find w as

$[x, y] = \text{hyperchaos2}d(x, y, a, b, k, r)$//equation (1)

$u = x + y$

$w = \text{floor}(u \times 10^{14})\text{mod}(256)$

(3) Add w to $s$box if it does not exist already in it

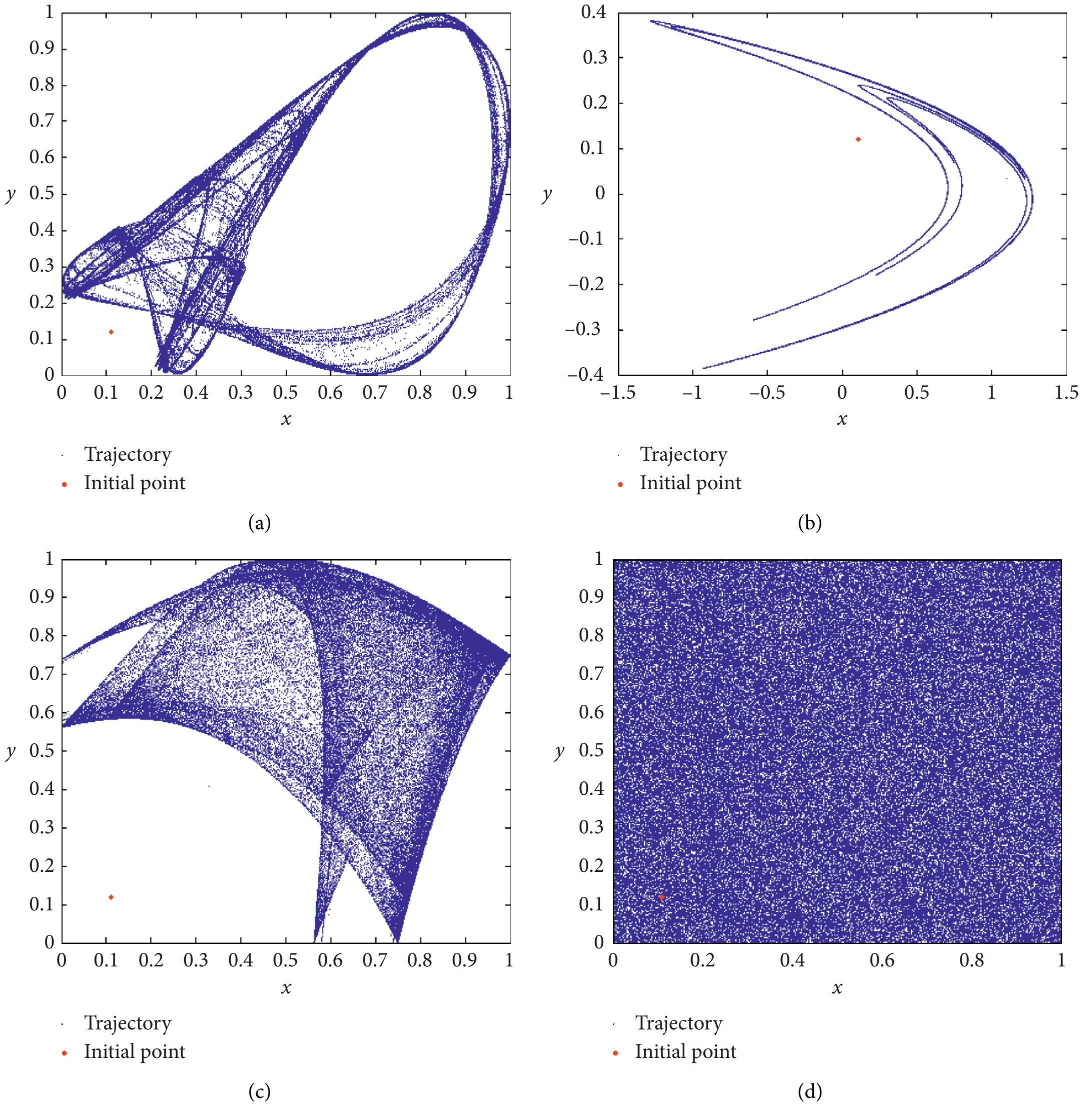
(4) Check if length $(s\text{box}) = 256$ and then exit. Else repeat from Step 2

The second phase evolves the initial S-box from phase-1 on the basis of average nonlinearity score. The evolution of S-box is based on the concept of random permutation matrix whose multiplication with a bijective S-box preserves its bijectivity. The change due to permutation matrix multiplication is accepted only when it causes some improvisation on the nonlinearity score of S-box. The algorithmic steps of phase-2 are subsequently given below. A simple example is also prepared to understand the effect of multiplying with random permutation matrix P.

Phase 2:

Require: Last chaotic variable x and y from phase-1, initial S-Box $s$box, gen_count
Return: S-Box $s$box_g

```
Set
$s\text{box}\_g = s\text{box}\_p =$
$\text{reshape}(s\text{box}, 16, 16) and\ find\ nl\_g =$
$\text{Nonlinearity}(s\text{box}\_g)$
while (gen_count > 0)
  $P = \text{zeros}(N, N)//N = 16$
  for $k = 1$ to $N$
    $[x, y] = \text{hyperchaos2}d(x, y, a, b, k, r)$
    $uu(k) = x + y$
  endfor
  $qq = \text{sort}(uu)$ and $T =$
  for $k = 1$ to $N$
    $t = qq(k)$
    find index $w$ in $uu$ such that $uu(w) = t$
    Set $T(k) = w$
  endfor
```



(a)

(b)

(c)

(d)

Figure 5: Phase portrait of chaotic attractor in 2D chaotic (a) logistic map, (b) Henon map, (c) SLMM map, and (d) proposed hyperchaotic map.

```
for $k = 1$ to $N$
    $P(k, T(k)) = 1$
endfor
$sbox\_p = (((sbox\_p) \times P)') \times P$
$nl\_p = \text{Nonlinearity}(sbox\_p)$
if $(nl\_p > nl\_g)$
    $sbox\_g = sbox\_p$
    $nl\_g = nl\_p$
endif
$\text{gen\_count} = \text{gen\_count} - 1$
endwhile
```

An example of the phase-2 procedure is illustrated, which is given in the Appendix for better apprehension. Phase-2 of the presented method resulted in an intermediate S-box given in Table 2.

third phase aims to explore the merits of algebraic technique to generate cryptographically near-optimal configuration of 8×8 S-box. To solve the purpose, a suitable algebraic group structure is constructed after exhaustive experimental analysis. It has been found that algebraic structure described below is the most suitable one among all those studied during our experimentation. The action of the obtained algebraic group structure gives the final proposed 8×8 S-box.

Phase 3:

Require: S-box *sbox_g* and algebraic group structure G
Return: final S-box S
Now, we apply the action of a group of permutations of order 841724928.

$$C_{346104} \times C_{152} \times C_4 \times C_2 \times C_2 = s, t, u, v, w, x,$$

The group G: $C_{346104} \times C_{152} \times C_4 \times C_2 \times C_2$ can be generated by 6 elements, namely s, t, u, v, w and x. Where,

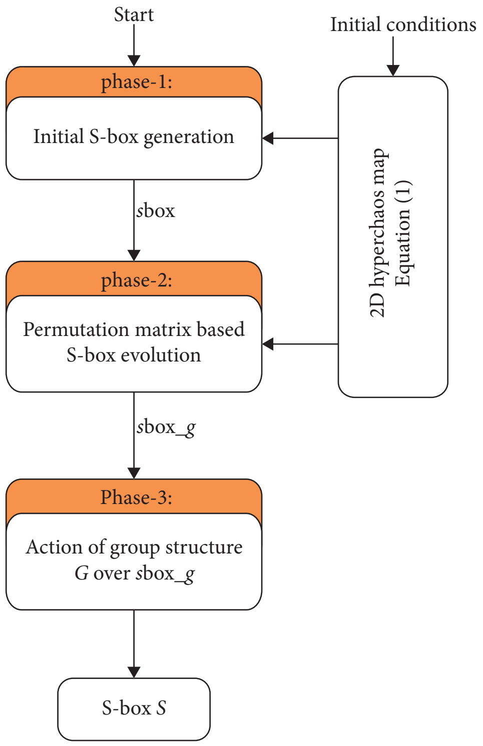

Start
Initial conditions
phase-1:
Initial S-box generation
sbox
phase-2:
Permutation matrix based S-box evolution
sbox_g
Phase-3:
Action of group structure G over sbox_g
S-box S
2D hyperchaos map Equation (1)

Figure 6: Block diagram of proposed S-box generation method.

Table 2: Intermediate S-box after phase-2.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	219	253	248	0	209	115	254	81	20	142	149	74	95	125	49	132
1	217	23	7	94	246	31	77	79	193	140	123	154	4	138	244	59
2	163	6	106	222	146	90	178	55	152	3	26	109	34	100	224	51
3	242	184	171	200	194	40	129	18	73	46	243	226	252	24	165	215
4	122	43	162	93	32	5	237	186	141	139	19	96	232	159	113	85
5	160	228	214	117	176	88	150	58	212	131	64	78	196	102	14	198
6	136	92	29	240	104	225	221	111	75	33	210	216	202	103	166	50
7	16	128	97	135	11	137	251	107	68	151	57	25	208	62	2	239
8	42	53	124	86	173	250	87	60	12	144	84	47	36	191	218	227
9	147	69	157	10	101	98	71	170	195	241	161	116	130	38	172	83
10	148	203	235	192	180	205	27	1	174	44	82	182	63	67	66	70
11	28	72	168	175	91	238	65	39	230	199	234	8	105	22	76	45
12	13	48	164	134	35	120	99	187	133	143	197	206	231	190	255	89
13	41	249	179	112	121	156	169	201	17	181	188	245	223	80	155	30
14	110	108	213	126	119	52	21	211	9	185	207	233	183	204	158	54
15	61	236	189	37	114	177	145	118	167	153	15	229	220	127	56	247

s = (1, 17, 149, 90, 137, 82, 217, 180, 68, 125, 227, 172, 161, 129, 187, 212, 157, 256, 185, 240, 37, 45, 161, 129, 187, 212, 157, 256, 185, 240, 37, 45, 106, 61, 50, 28, 194, 193, 201, 218, 60, 146, 236, 6, 23, 103, 127, 204, 177, 13, 56, 158, 94, 253, 245, 118);
t: = (2, 233, 31, 150, 191, 91, 207, 80, 190, 24, 211, 154, 251, 222, 225, 43, 153, 83, 231, 111, 44, 165, 34, 18, 242, 216, 38, 239, 210, 85, 167, 5, 156, 10, 184, 135, 136, 96, 42, 112, 197, 203, 200, 47, 51, 219, 27, 252, 188, 244, 109, 97, 208, 174, 205, 75, 148, 99, 170, 79, 169, 59, 234, 86, 122, 139, 155, 35, 89, 70, 248, 52, 67, 250, 115, 71, 238, 145, 92, 151, 144, 179, 76, 116, 213, 224, 140, 120);
u: = (3, 62, 138, 195, 226, 11, 98, 235);
v: = (4, 84, 214, 209, 123, 246, 29, 141, 87, 199, 130, 108, 102, 8, 198, 168, 95, 230, 66, 132, 57, 189, 88, 48, 162, 171, 40, 176, 81, 72, 229, 77, 78, 133, 113, 249, 36,

9, 65, 223, 196, 110, 160, 237, 54, 22, 46, 63, 166, 178, 114, 121, 32, 202, 55, 142, 26, 143, 21, 159, 232, 74, 49, 173, 14, 105, 12, 101, 20, 30, 19, 58, 247, 41, 39, 255);
w: = (7, 206, 100, 134, 33, 181, 15, 221, 107, 186, 192, 53, 215, 16, 73, 175, 163, 25, 147);
x: = (64, 93, 124, 220, 164, 152, 131, 228, 119, 104, 126, 69, 182, 183, 254, 128, 243, 241);

The action of each element/permutation on *s*box_*g* (obtained after phase-2, shown in Table 3) yields an S-box. After comprehensive analysis and study, it has been determined that the generated S-box S corresponding to permutation $s^3t^{35}u^7v^{29}wx^{13} \in C_{346104} \times C_{152} \times C_4 \times C_2 \times C_2$ was found to have strong cryptographic features. It acts on the indices of *s*box_*g*. The action of each element of said permutation of group G on the index set of *s*box_*g* gives distinct cryptographically sound S-box. We declare this S-box as our proposed S-box S which is shown in Table 3.

4. S-Box Performance Results

The significance of cryptographically sound S-box is that if it is not strong it means cipher has to suffer on the quality of encryption and security [51]. Therefore, before using any S-box in a cryptosystem, it is important to measure its security strength and robustness. A secure S-box should take care of the performance criteria well; for example, it should have balanced component Boolean functions, nonlinearity of components functions which must be high, satisfaction of SAC and BIC criteria, low differential uniformity, and linear approximation probability to resist linear cryptanalysis and differential cryptanalysis [20, 21]. In what follows, we discussed and assessed these performance parameters for our S-box and analyzed its security strength.

4.1. Nonlinearity. Nonlinearity property is a measure of dissimilarity between a function and its closest affine function. Since S-boxes are represented using Boolean functions, the nonlinearity of these functions becomes an important factor to measure the cryptographic strength of the S-boxes. Because linear functions can be easily breakable, it is prudent for S-boxes to generate efficient nonlinear functions. There should be sufficient nonlinear mapping of input to output and the S-box strength depends upon the value of nonlinearity which provides resistance against linear cryptanalysis [21]. In practice, the nonlinearity of a function F: $\{0,1\}^8 \longrightarrow \{0,1\}^8$ is computed using equation (8).

The nonlinearity of the S-box is determined by computing the nonlinearity of its component Boolean functions. We get scores such as 110, 112, 112, 110, 110, 110, 112, and 108 as nonlinearity of its component Boolean functions. The average nonlinearity of proposed S-box is 110.5 with least value of 108 and largest value of 112. The nonlinearity scores of proposed S-box are also shown graphically in Figure 7:

$$\mathrm{NL} = 2^7 - \frac{1}{2} \max_{v \in F_2^8,\, w \in F_2^8} \left| \sum_{x \in F_2^8} (-1)^{v.F(x)+w.x} \right|. \quad (8)$$

4.2. Strict Avalanche Criterion (SAC). Strict avalanche criterion was introduced by Webster and Tavares in 1985 to generalize the avalanche effect. According to SAC analysis, a single toggle in the input bit should alter 50% of the entire output bits to qualify as a suitable Boolean encryption function [52]. Hence, a good measure of SAC value makes the function show a strong random behaviour, making it complicated for attackers. In order to measure the SAC of S-box, dependence matrix is used. If value of each element in the dependence element as well its mean is close to 0.5, we can confirm that the S-box fulfils the strict avalanche criterion. The dependency matrix given in Table 4 is obtained using the procedure suggested in [52]. The SAC of the proposed S-box is found to be 0.5046 which is significantly close to ideal value of 0.5.

4.3. Bits Independence Criterion (BIC). Webster and Tavares also introduced another crucial criterion called output bits independence criterion of Boolean function. Pairwise independence of the avalanche variables for a given set of avalanche vectors is measured in order to determine nonlinearity of obtained functions [53]. The degree of independence between the pairs is measured through correlation coefficient. For the Boolean functions $g_0, g_1, \ldots, g_{n-1}$ to satisfy BIC, each Boolean function g_j xor g_k $(j \neq k, 0 \leq j, k \leq n-1)$ should have high nonlinearity to ensure sufficient independence. The BIC results for nonlinearity of our S-box are determined, which are presented in Table 5. The table shows the minimum nonlinearity of 102 but a high mean score of 109.14.

4.4. Differential Uniformity (DU). Differential cryptanalysis proposed by Biham and Shamir [54] and other related techniques are powerful tools to analyze block ciphers. It led to various research works exploring the security offered by different types of functions. Now, differential uniformity (DU) is used to find robustness of S-boxes against differential cryptanalysis as suggested in [54]. It is a measure of change observed in differential output Δb with respect to change in input Δa. In order to avoid these attacks, S-boxes with low values of DU are desirable. The expression given in equation (9) is used to compute DU for an S-box. Following the expression, we get the differential distribution table given in Table 6. Interestingly, the maximum value of the differential distribution table is 8 only. The remarkable feature of the S-box is that this maximum value of DDT (which is 8) occurs in the table only once:

$$\mathrm{DU}(S) = \max_{\Delta a \neq 0, \Delta b} \left(\#\{a \in S | S(a) \oplus S(a \oplus \Delta a) = \Delta b\}\right). \quad (9)$$

4.5. Linear Approximation Probability (LAP). Linear approximation probability is another vital security measure used to assess robustness of an S-box against Matsui's linear cryptanalysis [55]. This test is conducted to find imbalance of an event. The parity of the input bits selected by mask a is equal to the parity of output bits selected by mask b. According to Matsui's definition, linear approximation probability is measured as

Table 3: Proposed S-box after phase-3.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	220	67	24	165	121	226	157	211	150	47	92	20	2	167	91	169
1	114	204	103	155	186	14	69	185	235	70	241	33	143	134	19	51
2	250	237	116	36	247	71	31	152	40	98	212	153	230	52	22	7
3	173	34	79	60	45	1	82	206	104	83	90	13	146	144	43	170
4	99	75	198	228	189	39	35	0	132	159	109	229	156	41	236	174
5	56	101	118	205	96	249	191	138	142	219	44	224	124	95	63	244
6	195	207	6	190	122	172	233	127	222	54	223	246	26	225	162	76
7	177	105	50	8	11	102	65	89	58	176	68	126	17	239	115	25
8	213	218	32	74	57	240	253	9	217	164	27	136	129	55	160	188
9	187	133	193	180	137	10	171	62	5	151	209	30	42	28	119	81
10	208	46	66	111	97	86	135	242	201	23	145	93	16	21	141	178
11	221	73	123	12	163	61	215	107	112	210	182	80	94	243	29	199
12	184	252	108	216	64	139	140	85	154	203	255	77	166	254	113	214
13	128	168	88	148	37	72	194	78	131	48	179	251	49	161	53	202
14	106	149	175	238	117	125	200	232	231	158	248	181	120	197	227	130
15	192	147	245	110	38	59	183	87	4	3	84	15	18	196	100	234

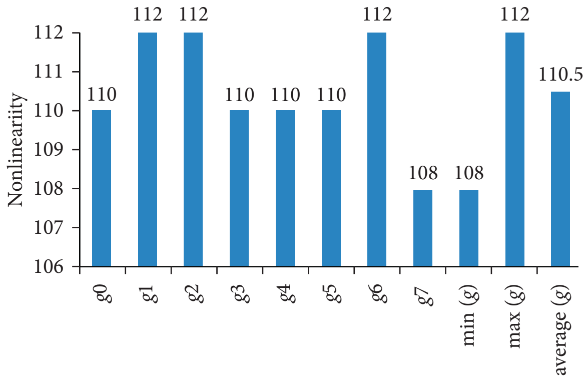


Figure 7: Nonlinearity scores of component Boolean functions of the proposed S-box.

Table 4: Dependency matrix for proposed S-box's SAC assessment.

	0	1	2	3	4	5	6	7
$g0$	0.4687	0.5312	0.5468	0.5468	0.4843	0.4687	0.5156	0.4531
$g1$	0.5	0.5312	0.5625	0.4843	0.4531	0.5156	0.4843	0.4843
$g2$	0.5468	0.5312	0.4843	0.5	0.5156	0.5312	0.5468	0.4531
$g3$	0.5468	0.4843	0.5	0.5156	0.4843	0.5156	0.4531	0.4531
$g4$	0.4843	0.4843	0.5156	0.5781	0.5625	0.4843	0.4375	0.5312
$g5$	0.5	0.5312	0.5468	0.4687	0.5	0.5156	0.5312	0.5156
$g6$	0.5	0.5625	0.5	0.4687	0.4687	0.5156	0.4531	0.5468
$g7$	0.5468	0.5	0.4687	0.5312	0.5312	0.4687	0.4531	0.5

Table 5: Nonlinearity scores of pairwise independent Boolean functions for BIC analysis of proposed S-box.

	$g0$	$g1$	$g2$	$g3$	$g4$	$g5$	$g6$	$g7$
$g0$	—	112	110	112	112	110	110	106
$g1$	112	—	110	110	110	110	112	106
$g2$	110	110	—	112	110	112	108	104
$g3$	112	110	112	—	110	112	110	106
$g4$	112	110	110	110	—	110	110	102
$g5$	110	110	112	112	110	—	110	104
$g6$	110	112	108	110	110	110	—	106
$g7$	106	106	104	106	102	104	106	—

Table 6: Differential distribution table for proposed S-box.

4	4	4	4	4	4	4	4	6	4	4	4	4	4	6	6
6	4	4	4	4	6	4	4	4	4	4	6	6	4	6	4
6	4	4	6	6	6	6	6	4	4	4	8	6	4	4	4
4	4	4	6	4	4	6	4	4	4	4	4	4	4	6	6
6	4	4	6	6	4	4	6	6	6	4	6	6	6	6	4
4	6	4	4	4	4	6	4	4	4	4	4	4	4	4	6
4	4	6	4	4	4	6	6	4	4	6	4	4	4	4	6
4	4	4	6	6	4	4	4	4	6	4	4	6	6	4	4
4	4	6	6	6	6	4	4	6	4	6	6	4	4	4	6
4	6	4	4	4	4	4	6	4	4	4	4	4	4	4	4
6	4	6	6	4	4	6	4	6	6	4	6	4	4	4	4
4	4	6	4	6	6	4	4	4	6	4	4	4	4	6	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	6	6	4	6	6	6	4	6	4	4	6
6	4	4	4	4	4	4	4	4	6	4	6	4	6	4	6
4	4	6	4	4	4	4	4	6	4	4	4	4	4	4	0

Table 7: Performance comparison of proposed S-box with recent S-box methods.

Method	Nonlinearity			SAC	BIC-NL	DU	LAP
	Min	Max	Average				
Proposed	108	112	110.5	0.5046	109.14	8	0.1094
Ref. [13]	104	110	106	0.5039	103.38	10	0.1406
Ref. [17]	102	108	105	0.5029	102.9	12	0.1484
Ref. [19]	106	108	106.5	0.4990	103.57	10	0.1250
Ref. [20]	104	108	106.5	0.5037	102.85	10	0.1406
Ref. [25]	102	108	105.25	0.5037	102.6	10	0.1328
Ref. [56]	102	108	105.25	0.4907	102.35	10	0.1328
Ref. [57]	106	108	107	0.4972	103.5	10	0.1563
Ref. [58]	106	108	106.5	0.5046	104.14	10	0.1328
Ref. [59]	103	109	105.1	0.5061	103.6	10	0.1563
Ref. [60]	106	108	106.7	0.4957	103.5	10	0.1250
Ref. [61]	100	110	105.5	0.5	103.78	12	0.1250
Ref. [62]	100	108	105	0.5007	104.14	10	0.1328
Ref. [63]	96	104	100.5	0.4973	102.78	10	0.15625
Ref. [64]	104	108	106.75	0.5031	103.64	12	0.1484
Ref. [58]	106	108	106.5	0.5046	104.14	10	0.1328
Ref. [65]	96	108	102.25	0.5059	103.5	12	0.1250
Ref. [66]	104	110	106	0.4978	103.92	12	0.1563
Ref. [67]	108	110	108.75	0.4946	102.78	10	0.1328
AES	112	112	112	0.5058	112	4	0.0625
APA	112	112	112	0.4987	112	4	0.0625
Gray [68]	112	112	112	0.5058	112	4	0.0625
Prime [68]	94	104	99.5	0.5164	101.71	72	0.1328
Skipjack [68]	104	108	105.25	0.5026	104.14	12	0.1172
Xyi [68]	104	106	105	0.5023	103.78	12	0.1563

$$\mathrm{LAP}(S) = \frac{1}{2^n}\left(\max_{a,b\neq 0}\left|\#\{x \in X | x.a = S(x).b\} - 2^{n-1}\right|\right), \tag{10}$$

where a and b are input and output masks, respectively, and X is the set of all possible inputs and 2^8 for 8×8 S-box which is the number of its elements. An S-box with low LAP value is desirable as it can oppose various linear attacks. We evaluated the linear approximation probability of proposed S-box and we found it to be 0.1094.

4.6. Comparison with State-of-the-Art S-Box Methods. The performance of any new S-box technique should be gauged against the already investigated state-of-the-art S-boxes. Here, we compared the cryptographic features of our proposed S-box with some recent S-boxes methods in Table 7. It is quite clear from the comparison analysis made in Table 7 that the nonlinearity of the proposed S-box is sufficiently the highest, which is 110.5, and the smallest value of linear approximation probability is 0.1094; both performance scores indicate higher robustness of proposed S-box against linear cryptanalysis and other related attacks compared to all

S-boxes listed in Table 7. The proposed S-box also satisfies the SAC criterion as its score is considerably closer to ideal 0.5 value, and it also satisfies well the BIC performance of the proposed S-box for nonlinearity having a decent value of 109.14, which is the highest among all the BIC scores of the comparison table. Our proposed S-box performs extremely well in putting effort to mitigate the differential cryptanalysis as the differential uniformity is 8, which is the lowest of all DU listed in the table. Hence, the comparison analysis makes it quite evident that our generated S-box has excellent cryptographic features, which performs significantly better than many recent and state-of-the-art S-boxes available in the literature.

5. Conclusions

The security of chaos-based cryptographic algorithms significantly depends on the dynamical characteristics of employed chaotic maps or systems. The applied chaotic maps should not have the frail performance for a strong chaotic cryptosystem. Keeping this guideline in consideration, this paper firstly suggested a 2D discrete hyperchaotic map, which is found to have prominently better dynamical characteristics compared to some existing 2D discrete chaotic maps when assessed against chaotic sensitivity, Lyapunov exponent, bifurcation, approximate entropy, and so forth. The proposed hyperchaotic map has been applied to suggest a novel approach for generating 8 × 8 S-boxes based on multiplication operation of random permutation matrices obtained through chaotic sequences. The approach of evolving S-boxes using the chaotic permutation matrices determined the suitable configuration of S-box. The S-box cryptographic strength improvisation is progressed by the action of experimentally found potent algebraic group structure. The performance appraisal against the well-accepted criteria shows the excellent security features of proposed S-box. It has been found after comparison analysis that the obtained S-box has better cryptographic security, robustness, and power than many S-boxes recently investigated and constructed in the literature.

The future scope of the proposed study includes its investigation for the construction of varying sizes of $n \times m$ substitution-boxes. The evolution of S-boxes can be made based on the multiple performance criteria instead of only nonlinearity to make it cryptographically strong and robust against related assaults. The generated S-boxes can also be applied to design cryptographic primitives such as image encryption, information hiding, and cryptographic hashing.

Appendix

For the phase-2 of the proposed S-box method for a hypothetical scenario, we have the following 5 × 5-order matrix named $sbox\_p$ (readers note that this is not the 5 × 5 S-box):

$$
sbox\_p = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 \end{bmatrix}. \qquad (A.1)
$$

For the above 5 × 5 $sbox\_p$ matrix, one needs a 5 × 5 permutation matrix P. So, to generate a random permutation matrix P of size 5 × 5, the hyperchaos map (1) is iterated 5 times to get chaotic arrays x and y, which are obtained as given below. Following the phase-2 algorithms, the arrays uu and sorted sequence qq are derived. The arrays uu and qq help to get the permutation sequence T, which in turn resulted in a random permutation matrix P of size 5 × 5. The incorporation of alteration in the previous matrix $sbox\_p$ according to the rule $sbox\_p = \left(\left((sbox\_p) \times P\right)'\right) \times P$ gives rise to another changed matrix $sbox\_p$ but consisting of all the elements of the input matrix $sbox\_p$ as evident from the matrix obtained in the presented example:

$$
\begin{aligned}
x &= [0.261105755315484, 0.858825702647243, 0.163850142521255, 0.601977298436912, 0.015230243618218],\\
y &= [0.775401184918429, 0.221530836755418, 0.992413671540929, 0.790516771946924, 0.082090433193052],\\
\mathrm{uu} &= [1.036506940233913, 1.080356539402661, 1.156263814062184, 1.392494070383837, 0.097320676811270],\\
\mathrm{qq} &= [0.097320676811270, 1.036506940233913, 1.080356539402661, 1.156263814062184, 1.392494070383837],\\
T &= [5,\ 1,\ 2,\ 3,\ 4],\\
P &= \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix},\\
sbox\_p &= \left(\left((sbox\_p) \times P\right)'\right) \times P,
\end{aligned}
$$

$$
\begin{aligned}
s\text{box\_}p &= \left(\begin{bmatrix}1&2&3&4&5\\6&7&8&9&10\\11&12&13&14&15\\16&17&18&19&20\\21&22&23&24&25\end{bmatrix}\times\begin{bmatrix}0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\end{bmatrix}\right)^{T}\times\begin{bmatrix}0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\end{bmatrix},\\
s\text{box\_}p &= \begin{bmatrix}7&12&17&22&2\\8&13&18&23&3\\9&14&19&24&4\\10&15&20&25&5\\6&11&16&21&1\end{bmatrix}.
\end{aligned}
\tag{A.2}
$$

Proceeding further in similar fashion, the new configuration of $s\text{box\_}p$ obtained after 100th successive generation for the above example case is given as

$$
s\text{box\_}p = \begin{bmatrix}19&17&18&20&16\\9&7&8&10&6\\14&12&13&15&11\\24&22&23&25&21\\4&2&3&5&1\end{bmatrix}. \tag{A.3}
$$

Data Availability

The necessary data are included within the article.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] A. A. A. EL-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, "Efficient quantum-based security protocols for information sharing and data protection in 5G networks," *Future Generation Computer Systems*, vol. 100, pp. 893–906, 2019.

[2] A. T. Sadiq, A. K. Farhan, and S. A. Hassan, "A proposal to improve RC4 algorithm based on hybrid chaotic maps," *Journal of Advanced Computer Science & Technology*, vol. 6, no. 4, pp. 74–81, 2016.

[3] M. Alawida, J. S. Teh, D. P. Oyinloye, W. H. Alshoura, M. Ahmad, and R. S. Alkhawaldeh, "A new hash function based on chaotic maps and deterministic finite state automata," *IEEE Access*, vol. 8, pp. 113163–113174, 2020.

[4] M. Ahmad and O. Farooq, "Chaos based PN sequence generator for cryptographic applications," in *Proceedings of the 2011 International Conference on Multimedia, Signal Processing and Communication Technologies*, pp. 83–86, IEEE, Aligarh, India, December 2011.

[5] L. R. Knudsen and M. Robshaw, *The Block Cipher Companion*, Springer Science & Business Media, Berlin, Germany, 2011.

[6] A. Razaq, H. A. Al-Olayan, A. Ullah, A. Riaz, and A. Waheed, "A novel technique for the construction of safe substitution boxes based on cyclic and symmetric groups," *Security and Communication Networks*, vol. 2018, Article ID 4987021, ,2018.

[7] N. A. Azam, U. Hayat, and I. Ullah, "An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization," *Security and Communication Networks*, vol. 2018, Article ID 3421725, 2018.

[8] A. A. A. El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics & Laser Technology*, vol. 116, p. 92102, 2019.

[9] M. Ahmad, E. Al-Solami, A. M. Alghamdi, and M. A. Yousaf, "Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures," *IEEE Access*, vol. 8, pp. 110397–110411, 2020.

[10] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami, and W. Alhakami, "Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications," *IEEE Access*, vol. 8, pp. 116132–116147, 2020.

[11] F. Özkaynak and A. B. Özer, "A method for designing strong S-boxes based on chaotic Lorenz system," *Physics Letters A*, vol. 374, no. 36, pp. 3733–3738, 2010.

[12] Y. Tian and Z Lu, "S-box: six-dimensional compound hyperchaotic map and artificial bee colony algorithm," *Journal of Systems Engineering and Electronics*, vol. 27, no. 1, pp. 232–241, 2016.

[13] Ü. Çavuşoğlu, A. Zengin, I. Pehlivan, and S. Kaçar, "A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system," *Nonlinear Dynamics*, vol. 87, pp. 1081–1094, 2016.

[14] M. Ahmad, M. N. Doja, and M. M. S. Beg, "ABC optimization based construction of strong substitution-boxes," *Wireless Personal Communications*, vol. 101, no. 3, pp. 1715–1729, 2018.

[15] A. A. Alzaidi, M. Ahmad, H. S. Ahmed, and E. A. Solami, "Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map," *Complexity*, vol. 2018, 16 pages, 2018.

[16] X. Wang, A. Akgul, U. Cavusoglu, V.-T. Pham, D. Vo Hoang, and X. Nguyen, "A chaotic system with infinite equilibria and its S-Box constructing application," *Applied Sciences*, vol. 8, no. 11, p. 2132, 2018.

[17] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175–54188, 2020.

[18] D. Lambi¢, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box

design," *Nonlinear Dynamics*, vol. 100, Article ID 699711, 2020.

[19] W. Gao, B. Idrees, S. Zafar, and T. Rashid, "Construction of nonlinear component of block cipher by action of modular group PSL (2, $\mathbb{Z}$) on projective line PL (GF (28)," *IEEE Access*, vol. 8, 2020.

[20] N. Hematpour and S. Ahadpour, "Execution examination of chaotic S-box dependent on improved PSO algorithm," *Neural Computing and Applications*, pp. 1–23, 2020.

[21] I. Hussain, "True-chaotic substitution box based on Boolean functions," *The European Physical Journal Plus*, vol. 135, no. 8, pp. 1–17, 2020.

[22] A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, "Quantum inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Scientific Reports*, vol. 10, no. 1, p. 116, 2020.

[23] M. Ahmad and E. Al-Solami, "Evolving dynamic S-boxes using fractional-order hopfield neural network based scheme," *Entropy*, vol. 22, no. 7, p. 717, 2020.

[24] A. Razaq, H. Alolaiyan, M. Ahmad et al., "A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups," *IEEE Access*, vol. 8, pp. 75473–75490, 2020.

[25] H. A. Ahmed, M. F. Zolkipli, and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," *Neural Computing and Applications*, vol. 31, no. 11, pp. 7201–7210, 2018.

[26] J. Wang, B. Pan, C. Tang, and Q. Ding, "Construction method and performance analysis of chaotic S-box based on fireworks algorithm," *International Journal of Bifurcation and Chaos*, vol. 29, no. 12, Article ID 1950158, 2019.

[27] A. K. Farhan, R. S. Ali, H. R. Yassein, N. M. G. Al-Saidi, and G. H. Abdul-Majeed, "A new approach to generate multi *s*-boxes based on RNA computing," *International Journal of Innovative Computing, Information and Control*, vol. 16, pp. 331–348, 2020.

[28] A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," *IEEE Access*, vol. 8, pp. 150326–150340, 2020.

[29] M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar, and A. Razaq, "Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes," *IEEE Access*, vol. 8, pp. 39781–39792, 2020.

[30] M. Ahmad, M. N. Doja, and M. S. Beg, "A new chaotic map based secure and efficient pseudo-random bit sequence generation," in *Proceedings of the International Symposium on Security in Computing and Communication*, pp. 543–553, Springer, Bangalore, India, September 2018.

[31] M. Ahmad, E. Al Solami, X.-Y. Wang, M. Doja, M. Beg, and A. Alzaidi, "Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos," *Symmetry*, vol. 10, no. 7, p. 266, 2018.

[32] M. Ahmad, C. Gupta, and A. Varshney, "Digital image encryption based on chaotic map for secure transmission," in *Proceedings of the 2009 International Multimedia, Signal Processing and Communication Technologies*, pp. 292–295, IEEE, Aligarh, India, March 2009.

[33] A. K. Farhan, N. M. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder," *Entropy*, vol. 21, no. 10, p. 958, 2019.

[34] N. Tsafack, S. Sankar, B. Abd-El-Atty et al., "A new chaotic map with dynamic analysis and encryption application in internet of health things," *IEEE Access*, vol. 8, 2020.

[35] N. Tsafack, J. Kengne, B. Abd-El-Atty et al., "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Information Sciences*, vol. 515, pp. 191–217, 2020.

[36] M. R. Salman, A. K. Farhan, and K. A. Hussein, "Color image encryption depend on DNA operation and chaotic system," in *Proceedings of the 2019 First International Conference of Computer and Applied Sciences (CAS)*, pp. 267–272, IEEE, Baghdad, Iraq, December 2019.

[37] A. A. Abd EL-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, S. E. Venegas-Andraca, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in internet of things," *Optics & Laser Technology*, vol. 124, Article ID 105942, 2020.

[38] Z. Hua and Y. Zhou, "Exponential chaotic model for generating robust chaos," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019.

[39] G. Alvarez, J. M. Amigó, D. Arroyo, and S. Li, "Lessons learnt from the cryptanalysis of chaos-based ciphers," in *Chaos-Based Cryptography*, pp. 257–295, Springer, Berlin, Germany, 2011.

[40] A. A. Alzaidi, M. Ahmad, M. N. Doja, E. A. Solami, and M. M. S. Beg, "A new 1D chaotic map and β-hill climbing for generating substitution-boxes," *IEEE Access*, vol. 6, pp. 55405–55418, 2018.

[41] M. Alawida, A. Samsudin, and J. S. Teh, "Enhancing unimodal digital chaotic maps through hybridisation," *Nonlinear Dynamics*, vol. 96, no. 1, pp. 601–613, 2019.

[42] A. V. Tutueva, E. G. Nepomuceno, A. I. Karimov, V. S. Andreev, and D. N. Butusov, "Adaptive chaotic maps and their application to pseudo-random numbers generation," *Chaos, Solitons & Fractals*, vol. 133, Article ID 109615, 2020.

[43] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Optics & Laser Technology*, vol. 101, pp. 30–41, 2018.

[44] S. Strogatz, *Nonlinear Dynamics and Chaos: with Applications to Physics, Biology, Chemistry, and Engineering*, Westview Press, Boulder, CO, USA, 1994.

[45] J. A. C. Gallas, "Structure of the parameter space of the Henon map," *Physical Review Letters*, vol. 70, pp. 2714–2717, 1993.

[46] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015.

[47] M. Alawida, A. Samsudin, and J. S. Teh, "Enhanced digital chaotic maps based on bit reversal with applications in random bit generators," *Information Sciences*, vol. 512, pp. 1155–1169, 2020.

[48] S. Pincus, "Approximate entropy as a measure of system complexity," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 88, pp. 2297–2301, 1991.

[49] J. M. Yentes, N. Hunt, K. K. Schmid, J. P. Kaipust, D. McGrath, and N. Stergiou, "The appropriate use of approximate entropy and sample entropy with short data sets," *Annals of Biomedical Engineering*, vol. 41, no. 2, pp. 349–365, 2013.

[50] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019.

[51] A. Razaq, A. Ullah, and A. Waheed, "A novel technique to improve nonlinearity of substitution box without disturbing its mathematical properties," *Wireless Personal Communications*, vol. 111, pp. 2091–2105, 2019.

[52] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proceedings of the Advances in Cryptology—CRYPTO'85*, pp. 523–534, Santa Barbara, CA, USA, August 1985.

[53] C. Adams and S. Tavares, “The structured design of cryptographically good s-boxes,” *Journal of Cryptology*, vol. 3, pp. 27–41, 1990.

[54] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” in *Proceedings of the Advances in Cryptology-CRYPT0’90*, pp. 2–21, Santa Barbara, CA, USA, August 1990.

[55] M. Matsui, “Linear cryptanalysis method for DES cipher,” in *Proceedings of the Advances in Cryptology—EUROCRYPT’93*, pp. 386–397, Lofthus, Norway, May 1993.

[56] M. Ahmad, H. Haleem, and P. M. Khan, “A new chaotic substitution box design for block ciphers,” in *Proceedings of the 2014 International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 255–258, IEEE, Noida, India, February 2014.

[57] A. H. Zahid, M. J. Arshad, and M. Ahmad, “A novel construction of efficient substitution-boxes using cubic fractional transformation,” *Entropy*, vol. 21, no. 3, p. 245, 2019.

[58] N. A. Azam, U. Hayat, and I. Ullah, “Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field,” *Frontiers of Information Technology & Electronic Engineering*, vol. 20, no. 10, pp. 1378–1389, 2019.

[59] F. Özkaynak and S. Yavuz, “Designing chaotic S-boxes based on time-delay chaotic system,” *Nonlinear Dynamics*, vol. 74, pp. 551–557, 2013.

[60] F. Özkaynak, “Construction of robust substitution boxes based on chaotic systems,” *Neural Computing and Applications*, vol. 31, no. 3, 2017.

[61] A. Belazi and A. A. A. El-Latif, “A simple yet efficient S-box method based chaotic sine map,” *Optik-International Journal for Light and Electron Optics*, vol. 130, pp. 1438–1444, 2016.

[62] U. Hayat, N. A. Azam, and M. Asif, “A method of generating 8 × 8 substitution boxes based on elliptic curves,” *Wireless Personal Communications*, vol. 101, no. 1, pp. 439–451, 2018.

[63] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, “Secure data encryption based on quantum walks for 5G internet of things scenario,” *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, Article ID 118131, 2020.

[64] A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah, and A. Waheed, “A novel construction of substitution box involving coset diagram and a bijective map,” *Security and Communication Networks*, vol. 2017, Article ID 5101934, 16 pages, 2017.

[65] B. B. Cassal-Quiroga and E. Campos-Cantón, “Generation of dynamical S-boxes for block ciphers via extended logistic map,” *Mathematical Problems in Engineering*, vol. 2020, Article ID 2702653, 12 pages, 2020.

[66] A. K. Farhan, R. S. Ali, H. Natiq, and N. M. G. Al-Saidi, “A new S-box generation algorithm based on multistability behavior of a plasma perturbation model,” *IEEE Access*, vol. 7, pp. 124914–124924, 2019.

[67] T. Zhang, C. L. P. Chen, L. Chen, X. Xu, and B. Hu, “Design of highly nonlinear substitution boxes based on I-Ching operators,” *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3349–3358, 2018.

[68] I. Hussain, T. Shah, M. A. Gondal, and W. A. Khan, “Construction of cryptographically strong 8 × 8 S-boxes,” *World Applied Sciences Journal*, vol. 13, no. 11, pp. 2389–2395, 2011.